

Zero Trust 網路存取

Cloudflare Zero Trust，特別是 Access，可提高團隊生產力並降低風險，因為所有使用者都可存取您的自託管、SaaS 或非 Web 應用程式，而無需使用 VPN。

為混合式工作提供簡單安全的存取

網際網路原生 Zero Trust 網路存取 (ZTNA)

如今的分散式工作環境要求採用分散式安全方法。「邊界」不復存在，因此，傳統的遠端存取解決方案（如 VPN）無法滿足現代網路安全或效能預期。

ZTNA 透過不斷地逐個資源檢查精細環境（如身分識別和裝置狀態），無論裝置和位置為何，都能在任何使用者與應用程式之間提供簡單安全的存取。使用全新的方法後，網路安全與使用者體驗之間不再需要「平衡行為」。ZTNA 可同時提升二者來支援您的業務。

它還可讓組織更加敏捷，能夠更好地應對變化，無論是雲端遷移、併購活動還是快速創新和擴展。Cloudflare 是零信任或網路安全現代化策略的核心，能夠在我們可程式化的全球連通雲上提供 ZTNA。

80% 解決與使用 VPN 相關的遠端存取支援工單花費的平均時間減少[1]

72% 與以前的廠商相比，節省的每月原則設定持續時間[1]

68% 對簡化員工和承包商的驗證體驗產生的重大影響[1]

為您的業務提供現代化存取



增強使用者體驗

藉助現代化網路安全，讓內部部署應用程式感覺就像 SaaS 應用程式一樣，進而提升團隊生產力。淘汰緩慢而笨拙的VPN，員工不再投訴。



消除橫向移動

透過授予每項資源以相關內容為基礎的最低權限存取，而非網路層級存取，來降低網路風險，縮小受攻擊面。



輕鬆擴展 Zero Trust

藉由保護關鍵應用程式或風險最高的使用者群組，然後擴展網際網路原生 ZTNA 來保護整個企業，進而提高技術效率。

Access 的主要使用案例

安全的混合式工作

- ★ **VPN 擴充與取代** — Access 比傳統的 VPN 更快更安全。開始卸載關鍵應用程式，以獲得更好的安全性和終端使用者體驗。
- ★ **承包商存取** — 藉助無用戶端選項、社交 IDP 等來驗證協力廠商使用者（如承包商）。
- **開發人員存取** — 讓特殊權限技術使用者能夠安全存取關鍵基礎架構，而無需犧牲效能。

實現數位現代化

- **加速合併和收購** — 完全避免傳統的網路合併。與多個 IdP 整合，在併購期間提供每個應用程式的內部存取。
- **雲端遷移** — 在轉換期間（例如，將應用程式或身分目錄遷移至雲端）保持業務連續性。
- **防網路釣魚攻擊的 MFA** — 隨時隨地推出增強式驗證，如符合 FIDO2 規範的安全金鑰。

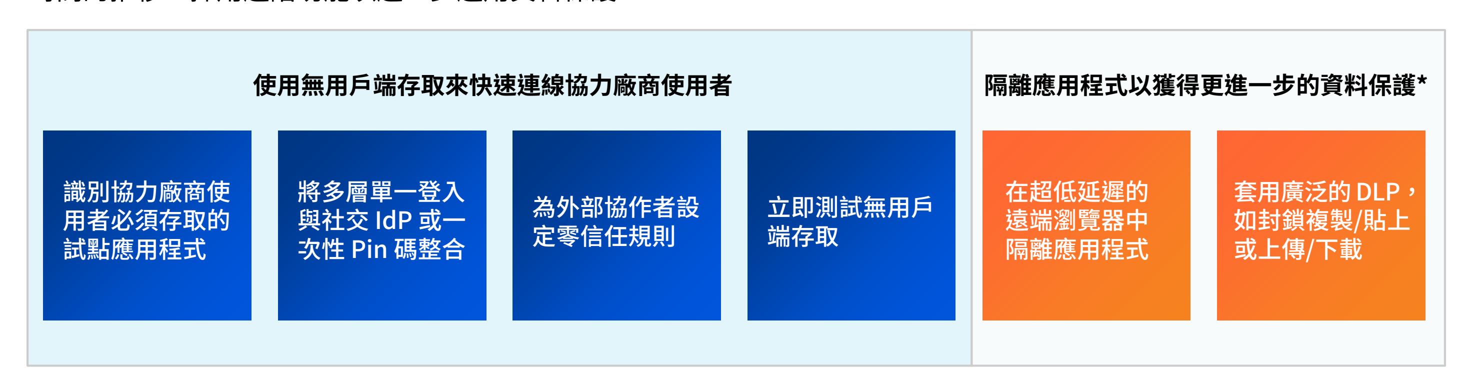
VPN 擴充與取代入門

優先安排關鍵應用程式或有風險的使用者進行 ZTNA 試點，以擴充您的 VPN。針對 Web 應用程式或瀏覽器內 SSH，使用無用戶端存取以加快測試。隨著時間的推移，採用進階功能以轉向完全取代 VPN，並隨著網路轉換保持動態可見性。



承包商（協力廠商）存取入門

提供順暢的使用者體驗，同時緩解來自未受管裝置的風險。為承包商設定簡單的驗證選項 — 無需終端使用者軟體。隨著時間的推移，採用進階功能以進一步運用資料保護。



在 Zero Trust 平台的其他部分使用功能

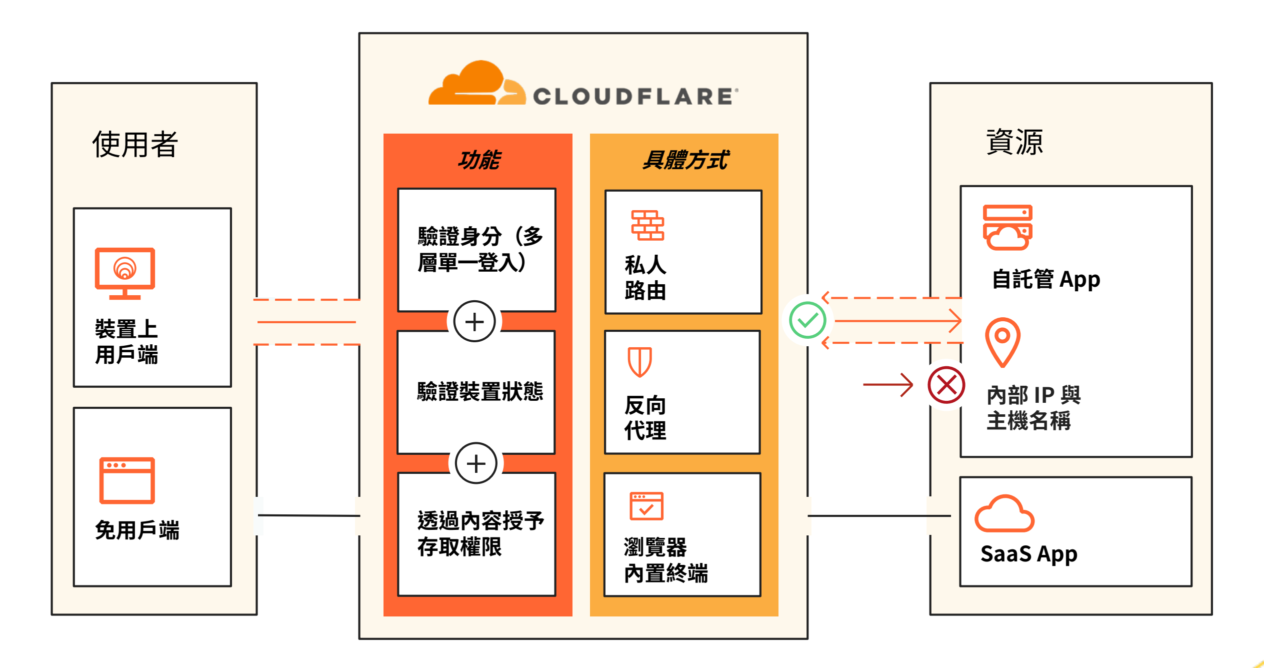
Access 運作方式

Cloudflare Access 是一個靈活的彙總層，它不斷地驗證精細環境（如身分識別和裝置狀態），來個別提供對組織所有資源簡單且安全的存取，從而建立軟體定義的邊界。當使用者進行驗證並符合所有存取原則準則時，Access 會核發一個已簽名的 JSON Web 權杖，在指定的工作階段持續時間內有效。我們透過組合式平台對所有使用者要求執行單遍檢查，並且由於我們獨特的 Anycast 網路架構，只需短短數秒，我們的集中式原則管理體驗就會讓原則變更在全球範圍內激增。

統一的無用戶端和基於用戶端的作業可處理所有裝置類型。我們針對所有零信任服務使用一個裝置用戶端，它會對我們的網路流量進行加密，來維護客戶資料的隱私權。我們還透過無用戶端設定，提供對企業外部裝置簡單且安全的存取。我們的 ZTNA、DNS 與市場領先的 WAF 和 DDoS 保護服務協同合作，共同建立並保護協力廠商使用者和混合員工在任意裝置上都可存取的公共主機名稱。我們的無使用者驗證選項（權杖或 mTLS 憑證）還解決了自動化服務和 IoT 裝置的使用案例。

對於零信任控制，資源會使用公共主機名稱反向代理自託管應用程式（雲端/內部部署）或瀏覽器內 SSH/VNC、身分識別代理 SaaS 應用程式，或基於用戶端/通道的私人路由透過第 4-7 層正向代理私有子網內的任何 Web 或非 Web（例如，任意 TCP/UDP）資源。我們的全球網路與應用程式連接器軟體相結合，支援任何運算環境（包括 Kubernetes 和容器在內的公有雲端，或者傳統的內部部署網路資源），既不需要 VM 基礎架構，也沒有輸送量限制，這與其他零信任廠商是不同的。

協力廠商身分識別、端點、網路入口、記錄/分析和 SIEM 工具與我們的裝置用戶端和分析的原生選項一起整合到我們的儀表板中，讓管理員能夠保持敏捷，並在他們已經使用的工具基礎上進行構建。



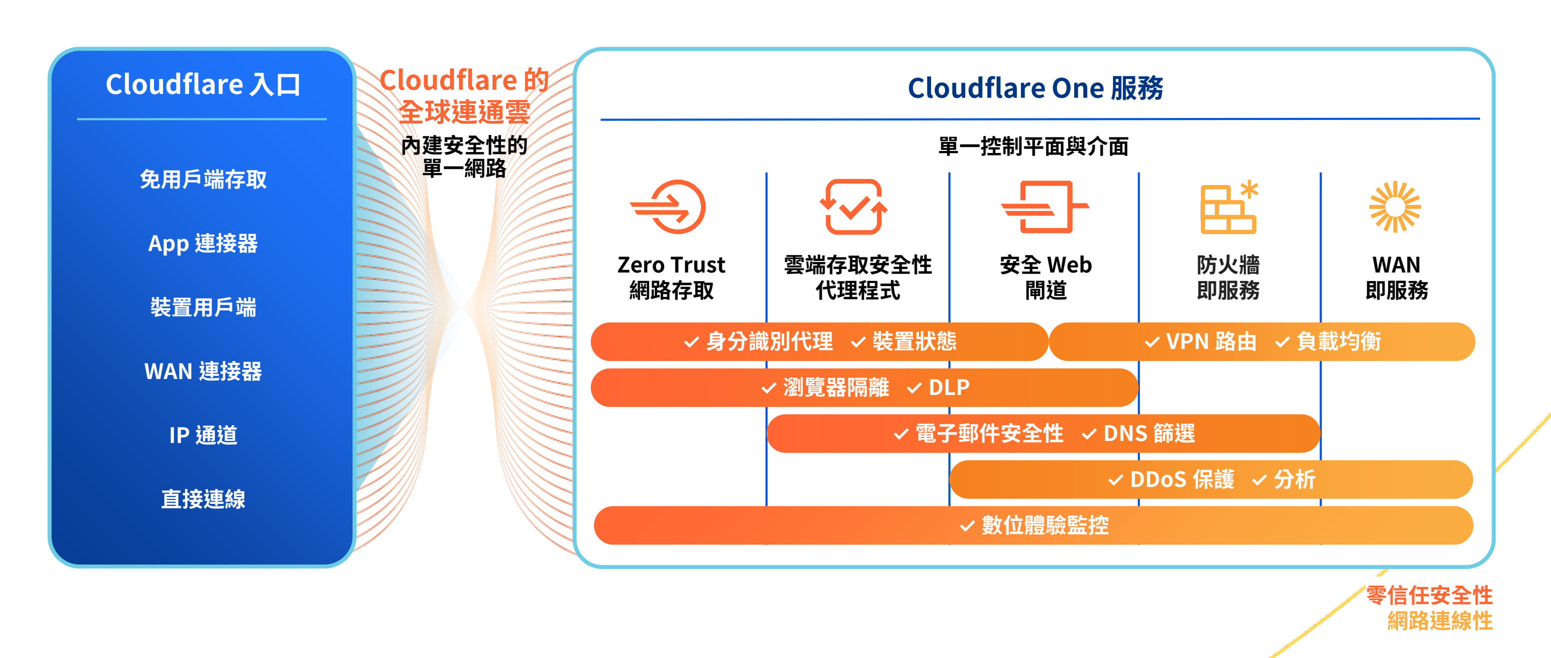
Access 是 Cloudflare 的 SSE 和 SASE 平台的一部分

雖然 SSE 和 SASE 通常涉及多年的策略旅程，但 Cloudflare 經常看到組織從 ZTNA 開始，因為 ZTNA 不僅包含 IT 團隊可執行且可達成的步驟，還展示出了顯著的短期商業價值。IT 領導者尋求在整合過程中保護混合式工作、抵禦威脅以及保護資料，因此越來越多地選擇 Cloudflare 作為他們信任的合作夥伴。

憑藉 Cloudflare 的部署靈活性和可組合架構，任何組織都能夠保護並加速裝置、應用程式乃至整個網路的效能，從而確保安全高效的混合式工作。為此，我們支援適用於終端使用者的無代理程式佈設、用於阻止不安全流量的無用戶端 Web 隔離，以及統一的管理儀表板，無論管理員或使用者從哪裡連線，都能查看所有安全性和網路服務。Cloudflare 全球網路的廣度支援在更靠近終端使用者的位置強制實施安全性，從而最大程度降低了延遲，並提供流暢的員工體驗。我們的 Anycast 架構有助於繞過網際網路中斷，從而確保團隊連線以及業務持續性。

使用我們統一的 SSE 和 SASE 平台，在 ZTNA、CASB、DLP 和 SWG 原則之間共用環境有助於增強安全狀態，同時透過一致的管理員工作流程來簡化實作。相同的身分識別和裝置狀態屬性可以通知 ZTNA 和 CASB 的存取原則以及 SWG 原則，從而簡化組織間的原則管理。

ZTNA、RBI 和電子郵件安全性也可以一起使用，從而有條件地存取資源，同時讓使用者免受在電子郵件和協作工具中看到的惡意內容（連結、附件）的影響。未受管裝置上的承包商和使用者可以有限地存取企業資源、透過停用使用者互動（例如，上傳/下載、複製/貼上、鍵盤輸入）來防止資料遭受入侵，並可套用其他第 7 層 DLP 原則來偵測敏感性資料。



客戶評價

「Cloudflare Access 是令人驚嘆的傳統 VPN 替代方案。使用者只要開啟瀏覽器並登入即可，不需要下載和設定其他軟體。」

— **Platzi**（雲端工程主管）

「在限制存取內部資產方面，Access 不僅比 VPN 簡單得多，也更加安全。我們只需啟用它並新增使用者即可。非常有效！」

— **Bitpanda**（技術長兼共同創辦人）

「Cloudflare Access 及時提供協助，讓我們免於經歷部署 VPN 的繁雜事務。這對我們而言是相當輕鬆的選擇，而且部署的簡易度相當驚人。」

— **ezCater**（網路安全主管）

「在我們實作 Cloudflare 之前，為安全部署準備一個應用程式需要兩到四週的時間。有了 Cloudflare Zero Trust，我們可節省 90% 的時間。」

— **Creditas**（網路工程團隊主管）

分析師的看法



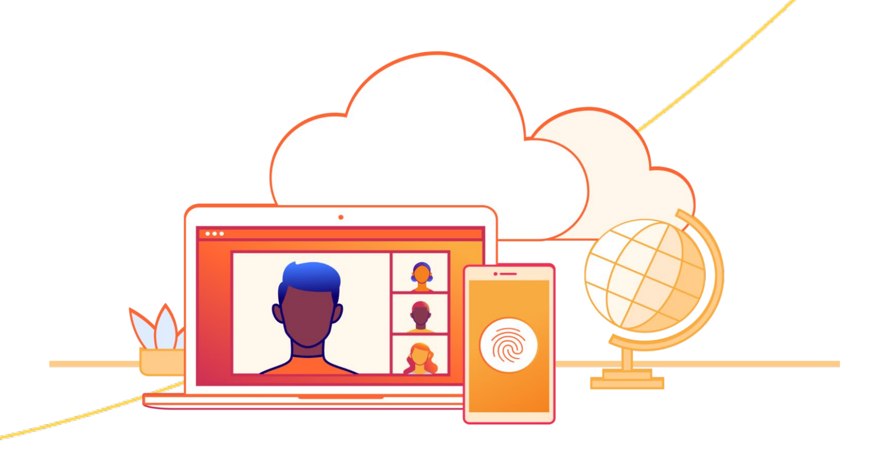
Cloudflare 在 2023 年 IDC MarketScape 中獲評為 Zero Trust 網路存取 (ZTNA)「領導者」

Cloudflare 因「積極的產品策略可支援企業安全需求」而獲得 IDC 的表彰。我們認為，我們獲得的表彰證明了我們的方法可以幫助任何規模的企業開始使用 Zero Trust，以及幫助任何使用者在沒有 VPN 的情況下安全存取任何資源。

kuppingercole
ANALYSTS

Cloudflare 在 2022 年 KuppingerCole Leadership Compass 中獲評為 ZTNA「領導者」

KuppingerCole Analysts AG 在 2022 年 ZTNA 市場分析中，列舉了 Cloudflare 的若干優勢，例如，完全整合且有機開發的網路安全平台、龐大的全球雲端基礎結構以及巨大的市場佔有率。



Access 功能

建立/編輯零信任原則以實現安全存取	
精細化自訂存取原則	集中式原則管理體驗。第 7 層應用程式獲得子網域和路徑層級的保護，以及萬用字元和多主機名稱支援，並支援 CORS 要求。只需短短數秒，原則變更就會在全球範圍內激增。包括原則測試器。
資源廣度： 我們保護的內容及方式	資源會使用公共主機名稱，在自託管應用程式（雲端/內部部署）或瀏覽器內 SSH/VNC 實作反向代理、在 SaaS 應用程式實作身分識別代理，或透過私有子網路內的第 4-7 層正向代理*任何 Web 或非 Web（例如，任意 TCP/UDP）資源，進行基於用戶端/通道的私人路由。
身分	透過所有主要企業和社交身分識別提供者 (IdP) 進行驗證，同時包括多個 IdP。此外還可以使用通用的 SAML 和 OIDC 連接器。支援（並可以強制執行）任何 IdP 提供的驗證方法、臨時驗證、目的證明、基於全球或每個應用程式工作階段的重新驗證間隔，以及每個應用程式或每個使用者的即時工作階段撤銷選項。
裝置狀態	使用裝置用戶端和協力廠商端點保護提供者 (EPP) 整合來驗證裝置狀態。使用服務到服務整合，將 EPP 風險評分納入零信任原則中。
原則的關聯式訊號	設定訊號，如電子郵件群組、IP 範圍、地理位置、登入方式（例如，MFA 類型、IdP 類型）、有效的 mTLS 或 SSH 憑證、服務權杖、序號清單、裝置狀態屬性、安裝的裝置用戶端、工作階段持續時間、SWG 規則強制執行或來自外部 API 呼叫的訊號。還可以直接參考 Microsoft Entra ID (Azure AD) 條件式存取原則。
其他相關支援	• **SCIM：**自動為自託管和 SaaS 應用程式（例如，Okta 和 Azure AD）佈建/取消佈建使用者 • **內部 DNS：**設定本機網域回復並解析私人網路要求 • **分隔通道：** 包括/排除 IP，用於建立私人網路或與 VPN 一起執行 • **mTLS 驗證：** 基於憑證的驗證，用於 IoT 和其他 mTLS 使用案例 • **應用程式隔離：**只需一個核取方塊，即可在我們快如閃電的遠端瀏覽器中隔離應用程式*
入口和出口	
App 連接器	簡單協調我們的輕量級應用程式連接器 (Cloudflare Tunnel)，可加速將資源連線至 Cloudflare，既不需要 VM 基礎架構，也沒有輸送量限制。包括監控、虛擬網路（針對 IP 重疊）以及備援和容錯移轉功能。
裝置用戶端： 何時使用	• **無用戶端：**將零信任原則擴展至未受管裝置上的協力廠商使用者；同時與無用戶端 RBI 和第 7 層 DLP 原則良好搭配*。無用戶端存取支援 Web 應用程式和瀏覽器內 SSH/VNC。 • **基於用戶端：**我們的裝置用戶端 (Cloudflare WARP) 將安全存取擴展至私人網路，支援服務到服務裝置狀態整合，並且能夠感知位置，以針對內部部署使用者套用定制原則。還可以連線任意兩個或更多執行 WARP 的裝置來建立私人網路。使用者可以自行註冊，也可以透過 MDM 進行部署。
可擴展性和可見度	
頁面自訂	上傳封鎖和應用程式啟動器畫面的自訂 HTML，來適應您的品牌形象或傳達特定的存取說明，從而簡化終端使用者體驗。
記錄	全面記錄所有要求、使用者和裝置。可以使用 logpush 或 API 與現有 SIEM、協調和分析工具整合。針對未知資產，我們用於內部基礎架構的影子 IT 會被動地將公開所有來源的獨特流量分類。
自動化	直覺化 API 和 Terraform 提供程式可用於以程式設計方式管理零信任實作的所有方面。還會為自動化服務提供無使用者服務權杖支援。

在 Zero Trust 平台的其他部分使用功能

為什麼選擇 Cloudflare？



輕鬆設定和管理

透過應用程式連接器軟體和通道協調流程，從根本上簡化私有資源入口流量的設定和作業。



順暢的永遠連線體驗

藉助 Cloudflare 的全球 Anycast 技術，實現終端使用者最高效能和網路服務中斷復原能力，從而確保可靠性。



早期採用者的快速創新

藉助提供者，在創新方面不斷地超過同儕，讓應用程式存取更快速、更安全，從而跟上網際網路本身的發展。

我們來討論一下適用於您組織的簡單安全的存取

申請研討會



尚未準備好開始一場即時交談？

不斷深入瞭解 **Cloudflare 的 SSE 和 SASE 平台**



1. 2023 調查：techvalidate.com/product-research/cloudflare/charts

+ 886 8 0185 7030 | enterprise@cloudflare.com | cloudflare.com